KLIK: Kajian Ilmiah Informatika dan Komputer
ISSN 2723-3898 (Media Online)
Vol 4, No 3, Desember 2023, Hal 1313-1322
DOI 10.30865/klik.v4i3.1423
https://djournals.com/klik

Sistem Keamanan E-Voting Menggunakan Arsitektur Publik Blockchain Ethereum

Abiyyu Yafi, Putra Prima Arhandi, Vipkas Al Hadid Firdaus*, Ade Ismail, Kadek Suarjuna Batubulan

Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Malang, Malang, Indonesia
Email: [1y]afiabiyyu@protonmail.com, [2]putraprima@polinema.ac.id, [3,*]vipkas@polinema.ac.id, [4]aismail@polinema.ac.id, [5]kadek@polinema.ac.id
Email Penulis Korespondensi: vipkas@polinema.ac.id

Abstrak−Pemilihan Umum merupakan sebuah prosedur dalam memilih pemimpin di sebuah negara demokrasi. Hanya saja, pada Pemilihan Umum rentan adanya manipulasi suara menjadi salah satu isu yang berkembang. Saat ini, sistem e-voting memungkinkan peretas untuk mengendalikan sistem dan merusak hasil pemilihan. Selain itu, sistem proses pemilihan yang tidak transparan sulit untuk diawasi bersama-sama. Dalam artikel ini diusulkan sebuah prototipe aplikasi pemilihan umum pada fase pencoblosan suara, pengumpulan hasil suara di setiap TPS dan rekapitulasi suara. Penelitian ini menggunakan konsep *blockchain* dengan platform Ethereum. Sistem e-voting yang dibangun menerapkan *smart contract* pada jaringan public Ethereum blockchain. Tujuannya adalah untuk menjaga keamanan data hasil pemilihan serta menjaga kerahasiaan pemilih dengan menggunakan alamat Ethereum yang mewakilkan satu pemilih. Selain itu, dengan menggunakan jaringan public blockchain Ethereum, proses pemilihan dapat diawasi secara bersama-sama. Adapun hasil yang didapatkan dalam penelitian yang dilakukan pada tulisan ini adalah memperlihatkan bagaimana penerapan *blockchain* dapat menjaga integritas data dengan menunjukkan nilai dari data tersebut.

Kata Kunci: Blockchain; Ethereum; Smart Contract; Pemilihan Umum; E-voting

Abstract−General elections are a procedure for selecting leaders in a democratic country. However, during the General Election, the vulnerability to vote manipulation is one of the growing issues. Currently, e-voting systems allow hackers to control the system and tamper with election results. In addition, an election process system that is not transparent is difficult to supervise jointly. In this article, a prototype of a general election application is proposed in the voting phase, collecting vote results at each polling station and vote recapitulation. This research uses the blockchain concept with the Ethereum platform. The e-voting system applies smart contracts on the public Ethereum blockchain network. The aim is to maintain the security of election results data and maintain voter confidentiality by using an Ethereum address that represents one voter. In addition, by using the Ethereum public blockchain network, the election process can be monitored jointly. The results obtained in the research conducted in this paper show how the application of blockchain can maintain data integrity by showing the value of the data.

Keywords: Blockchain; Ethereum; Smart Contract; General Election; E-voting

1. PENDAHULUAN

E-voting merupakan sistem pemungutan suara yang menggunakan teknologi elektronik seperti komputer, telepon, atau ponsel untuk menghitung suara pemilih. *E-voting* sendiri memiliki kelebihan dibandingkan proses pemilihan dengan menggunakan metode tradisional, dimana *e-voting* dapat mempercepat proses pelaksanaan pemilihan, mengurangi biaya dalam proses pemilihan dan meningkatkan tingkat akurasi dalam proses pemilihan[1], [2]. Penggunaan *e-voting* juga menimbulkan beberapa resiko, seperti krentanan terhadap serangan *cyber* dan masalah integritas data. Untuk mengurangi resiko tersebut, diperlukan tindakan pengamanan yang tepat. Beberapa penelitian berpendapat bahwa sistem *e-voting* masih memiliki permasalahan dalam menjaga keamanan data dan privasi dari pengguna, dimana sistem *e-voting* yang ada pada saat ini masih memungkinkan kejahatan serangan *cyber* untuk mengendalikan sistem *e-voting* dengan tujuan untuk menggangu jalannya proses pemilihan[3], [4]. Untuk mengurangi resiko tersebut, diperlukan tindakan pengamanan yang tepat seperti enkripsi data, autentikasi pemilih yang kuat dan pemantauan yang ketat terhadap sistem dengan menggunakan teknologi *blockchain.* Menurut penelitian yang dilakukan oleh [5] terdapat 120 potensi serangan terhaap sistem pemungutan suara yang dikelompokan menjadi beberapa kategori yaitu*:* (a) Malware Insertion yaitu potensi serangan yang pertama adalah malware insertion merupakan serangan yang menargetkan perangkat yang digunakan dalam sistem pemungutan suara, dimana pada penyerangan ini peretas memiliki akses pada sistem pemungutan suara yang bertujuan untuk memasukan program yang dapat merusak program pemungutan suara untuk menambahkan total suara dari salah satu kandidat dan juga membuat data hasil pemilihan dari pemilih menjadi tidak sah. Potensi serangan ini sangat sulit dilakukan secara efektif dikarenakan satu permasalahan yang ada, dimana potensi serangan ini harus dilakukan sebelum pelaksanaan pemungutan suara dilakukan. (b)Wireless and Other Remote-Control Attacks *yaitu* potensi serangan yang kedua merupakan jenis serangan yang mentargetkan perangkat yang digunakan dalam pemungutan suara, berbeda dengan potensi serangan malware insertion dimana potensi serangan ini dapat dilakukan sebelum ataupun saat proses pemungutan suara berlangsung. Penyerangan ini mentargetkan perangkat dalam pemungutan suara yang memiliki komponen nirkabel di dalamnya yang sangat rentang terhadap serangan, yang memungkinkan peretas untuk masuk kedalam sistem melalui perangkat nirkabel dan dapat mengendalikan perangkat yang digunakan dalam pemungutan suara dan juga memasukan malware yang bertujuan untuk membaca informasi yang direkam dan di simpan di dalam perangkat pemungutan suara. (c) Denial-of-Service (Dos) yaitu potensi serangan yang ketiga adalah denial-of-service (dos) merupakan salah satu jenis serangan yang memiliki cakupan yang luasdimana pada penyerangan ini bertujuan untuk menggangu komunikasi antara klien dan juga server yang digunakan dalam pemungutan suara, yang memiliki tujuan untuk membanjiri bandwidth kepada sistem yang di jadikan sebagai target dengan membuat lalulintas

komunikasi data melebihi dari batas yang dapat di tangani oleh sistem pemungutan suara yang bertujuan untuk mencegah pemilih memberikan hak suaranya. (d) Attacks on Counting Servers yaiyu potensi serangan berikutnya adalah attacks on counting servers, yang merupakan salah satu serangan yang memiliki target terhadap server yang berfungsi sebagai tempat penyimpanan data dari hasil perhitungan total suara yang didapat oleh masing-masing kandidat [6], [7]. Server yang digunakan sebagai tempat penyimpanan data hasil dari pemilihan dapat di serang secara langsung melalui database yang menyimpan data hasil pemilihan. Berdasarkan dua kasus yang pernah terjadi, peretasan memiliki tujuan untuk menghapus seluruh catatan pemungutan suara, melakukan perubahan suara yang akan di umumkan oleh server perhitungan suara ataupun mengubah seluruh informasi yang akan digunakan untuk menghitung seluruh total suara yang didapatkan oleh masing-masing kandidat.

Blockchain adalah sebuah sistem penyimpanan yang menyimpan data dalam bentuk blok yang terikat satu sama lain dengan menggunakan enkripsi[8]. Setiap block dapat menyimpan sejumlah data dan terikat dengan block sebelumnya melalui sebuah tautan yang disebut dengan *hash*, yang menciptakan sebuah rantai blok *(blockchain)* yang saling terikat dan tidak dapat diubah. *Blockchain* dapat digunakan untuk menyimpan berbagai jenis data, termasuk transaksi finansial, data medis, dan data pemilihan.keunggulan dari blockchain adalah transparansi dan keamanan yang tinggi, karena setiap blok pada rantai blok tersebut terproteksi dengan enkripsi yang kuat dan tidak dapat diubah, *blockchain* juga tidak membutuhkan pihak ketiga untuk melakukan validasi transaksi, sehingga proses transaksi menjadi lebih cepat dan efisien[9], [10].

Salah satu teknologi *blockchain* yang terkenal adalah *Ethereum* [11], [12]. *Ethereum* merupakan salah satu platform *blockchain* yang pertama kali diperkenalkan oleh Vitalik Butterin. *Ethereum* merupakan salah satu platform *blockchain* yang menyediakan lingkungan untuk menjalankan *smart-contract*. *Smart-contract* sendiri adalah sebuah kontrak digital yang ditulis dalam Bahasa pemrograman komputer dan dijalankan di atas *blockchain*[13]. *Smart-contract* memungkinkan pihak-pihak untuk mengatur hubungan kontraktual secara terotomatisasi tanpa perlu adanya pihak ketiga yang dipercaya sebagai mediator, *smart-contract* menggunakan aturan-aturan yang ditetapkan secara terperinci dalam kontrak untuk mengeksekusi transaksi atau mengambil Tindakan lain yang diperlukan di saat kondisi tertentu terpenuhi[14], [15].

Permasalahan pada sistem *e-voting* perlu diatasi dengan sebuah teknologi yang tentunya dapat menyelesaikan permasalahan *e-voting*, khususnya dalam menjaga keamanan data dari hasil pemilihan dan privasi dari pemilih. Salah satu teknologi yang dapat menanggulangi permasalahan pada sistem *e-voting* yaitu teknologi *blockchain*, teknologi *blockchain* memiliki karakteristik desentralisasi, transparan, dan tidak dapat dimodifikasi. Salah satunya adalah *ethereum blockchain*, merupakan infrastruktur komputasi yang terdistribusi dan desentralisasi. *Ethereum blockchain* merupakan salah satu *public blockchain* dimana semua orang dapat melihat dan juga menambahkan data kedalam jaringan public *blockchain*, dan *ethereum blockchain* juga dapat menjalankan program yang disebut dengan *smart-contract*[16], [17]. *Smart-contract* pertama kali diperkenalkan oleh Nick Szabo pada tahun 1997 dan di implementasikan di dalam *ethereum blockchain, smart-contract* pada *ethereum blockchain* merupakan sebuah perangkat lunak yang dijalankan oleh *ethereum virtual machin (evm)*, kode sumber dari *smart-contract* yang telah dibuat akan disimpan secara permanen di dalam *ethereum blockchain* dan kode sumber tersebut tidak dapat dirubah[18].

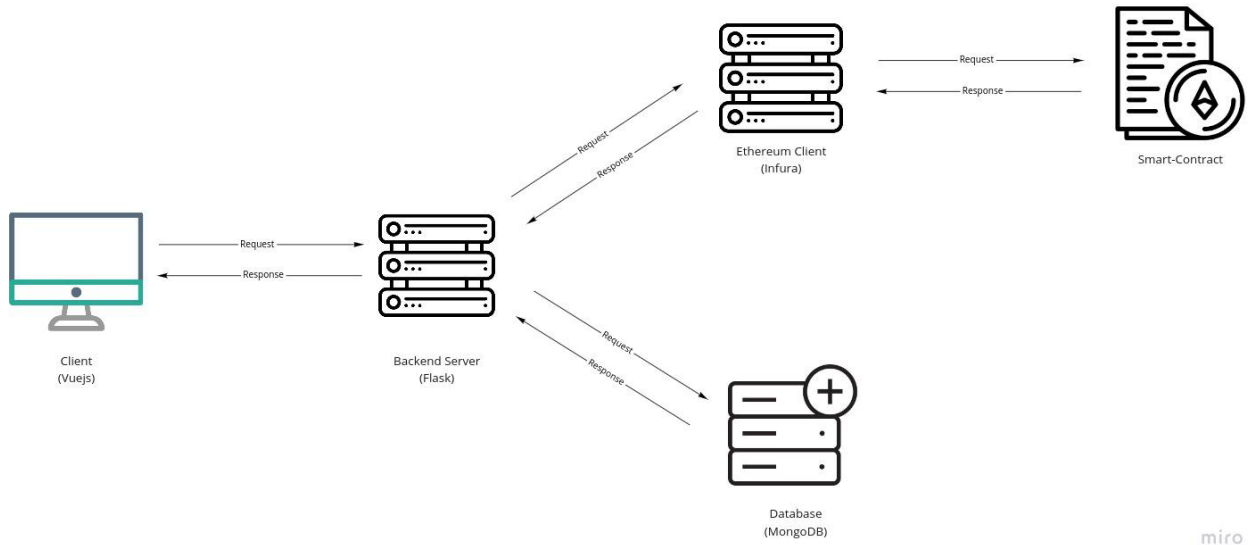
Menghadapi tantangan terkait keamanan, penting untuk menerapkan langkah-langkah keamanan yang efektif, dan teknologi blockchain muncul sebagai solusi yang menjanjikan. Blockchain adalah sistem penyimpanan data terdesentralisasi dan transparan di mana blok-blok terhubung melalui enkripsi, menciptakan rantai yang tidak dapat diubah. Ethereum, sebagai teknologi blockchain yang dikenal luas, memperkenalkan konsep smart contract. Smart contract adalah kontrak digital yang dieksekusi di blockchain, memungkinkan pihak-pihak untuk mengotomatiskan hubungan kontraktual tanpa memerlukan pihak ketiga yang dipercayai. Kontrak ini mengeksekusi aturan yang telah ditetapkan ketika kondisi tertentu terpenuhi, memberikan kerangka kerja yang aman dan transparan.

Permasalahan pada sistem e-voting, khususnya terkait keamanan data pemilihan dan privasi pemilih, memerlukan solusi teknologi yang tepat. Teknologi blockchain, dengan karakteristik terdesentralisasi, transparan, dan tidak dapat dimodifikasi, menawarkan solusi yang dapat diandalkan. Ethereum blockchain, sebagai blockchain publik, memungkinkan siapa pun untuk melihat dan menambahkan data ke jaringan. Lebih lanjut, dapat mengeksekusi smart contract yang, setelah diimplementasikan, tetap tersimpan secara permanen dan tidak dapat diubah. Tujuan dari penelitian ini adalah mengusulkan penerapan smart contract dalam Ethereum blockchain untuk mengatasi masalah keamanan dan privasi dalam sistem e-voting, dengan tujuan menyediakan lingkungan pemungutan suara yang kokoh dan aman [19].

2. METODOLOGI PENELITIAN

2.1 Deskripsi Sistem

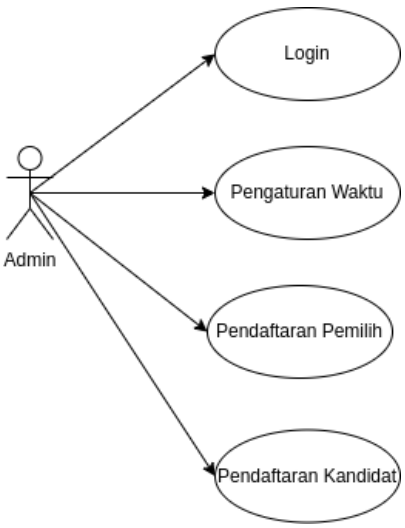
Sistem e-voting yang dibangun dengan menerapkan konsep blockchain [20]. Sistem dibangun dengan berbasis website dengan menerapkan *smart-contract* yang dibangun diatas *ethereum blcockhain*. Sistem *e-voting* menggunakan 2 tempat penyimpanan yang berbeda yaitu dengan menggunakan *smart-contract* sebagai tempat penyimpanan data hasil pemilihan dan juga tempat penyimpanan hak akses dari setiap pengguna sistem *e-voting*. *Database mongodb* digunakan untuk menyimpan data yang bersifat rahasia dari data pemilih dan juga kandidat sehingga data tersebut tidak dapat di akses melalui jaringan *public blockchain* [21].



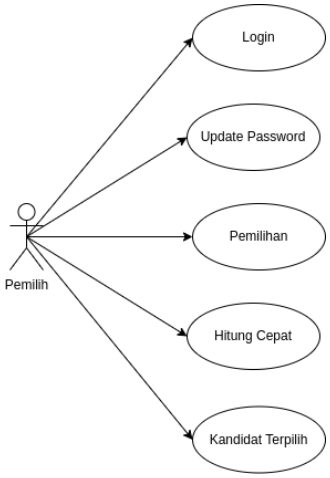
Gambar 1. Arsitektur Sistem

Berdasarkan arsitektur sistem pada Gambar 1 berikut ini adalah penjelasan mengenai arsitektur sistem yang dibuat pada penelitian ini:

a. Client
   Client yang terdapat di dalam arsitektur sistem akan dibuat berbasis website dengan menggunakan vuejs framework, client akan ditempatkan di salah satu infrastructure as a service (IaaS) yaitu Microsoft azure.
b. Backend server
   Backend server yang akan dikembangkan dalam penelitian ini menggunakan bahasa pemrograman python dengan menggunakan salah satu framework yaitu flask, dimana tugas dari backend server akan dijadikan sebagai web service yang berfungsi untuk mengirim dan menerima data dari client dan juga smart-contract. Backend server akan ditempatkan ditempat yang sama seperti client yaitu microsfot azure.
c. Database
   Database yang akan digunakan dalam penelitian ini adalah mongodb salah satu database NoSQL, tugas dari database pada sistem e-voting adalah untuk menyimpan data dari pengguna sistem e-voting. Database nantinya akan menggunakan salah satu Database as a service (DBaaS).
d. Smart-contract
   Smart-contract pada penelitian ini dibuat dengan menggunakan bahasa pemrograman solidity salah satu bahasa pemrograman yang digunakan dalam pembuatan smart-contract, serta menggunakan salah satu framework untuk membuat sebuah smart-contract pada ethereum blockchain yaitu truffle.
e. Infura
   Infura merupakan layanan penyedia application programming interface (api) untuk terhubung dengan jaringan ethereum sehingga dapat mempermudah dalam penelitian dengan memanfaatkan api yang telah disediakan oleh infura.



Gambar 3. Usecase Admin

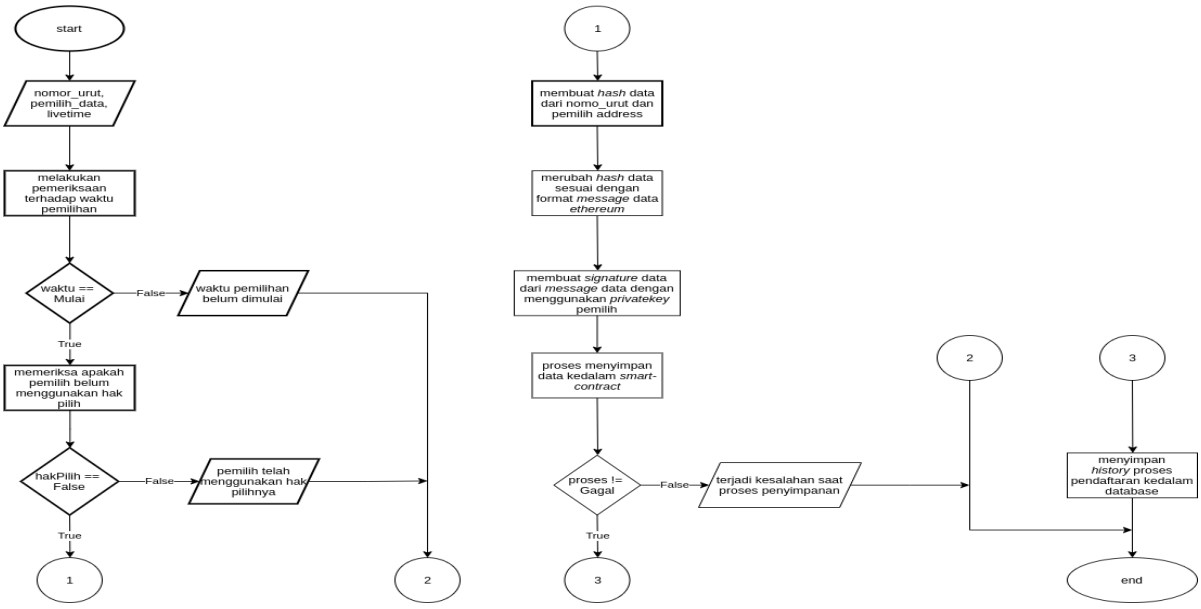


Gambar 4. Usecase Pemilih

Pada Gambar 3 dan Gambar 4 merupakan *use case* diagram dari sistem *e voting* yang menjelaskan kegiatan yang dilakukan oleh pengguna dari sistem *e-voting.* Sistem *e-voting* memiliki 2 pengguna yaitu *admin* dan pemilih. Berikut ini adalah penjelasan dari Gambar 3 dan Gambar 4:

a. Admin
   Admin adalah pengguna yang memiliki akses untuk mengatur tanggal dan waktu yang menentukan kapan proses pendaftaran dan pemilihan dapat dilakukan di dalam sistem *e-voting*. *Admin* juga dapat mendaftarkan pemilih dan kandidat yang mengajukan pendaftaran kepada *admin* dengan syarat tanggal dan waktu yang telah ditentukan sebelumnya.
b. Pemilih
   Pemilih adalah pengguna yang akan memberikan hak pilihnya kepada kandidat yang telah terdaftar di dalam sistem *e-voting*, dimana pemilih diharuskan untuk mendaftarkan dirinya terlebih dahulu agar dapat memerikan hak pilihnya kepada kandidat yang akan di pilih. Pemilih juga dapat melihat perhitungan sementara dari total suara yang didapatkan dari masing masing kandidat yang terdaftar di dalam sistem *e-voting* sehingga akan mengetahui perolehan sementara dari total suara dari masing-masing kandidat, pemilih juga dapat melihat pemenang dari pemilihan jika proses pemilihan telah ditutup. Pemilih juga dapat melakukan perubahan *password* untuk menjaga agar akun dari pemilih tetap aman.

Selanjutnya Pada Gambar 5 merupakan proses dari pemilihan kandidat yang dilakukan oleh pemilih, dimana sistem akan melakukan pemeriksaan terhadap tanggal beserta waktu apakah proses pemilihan telah dimulai, berikutnya sistem akan melakukan pemeriksaan terhadap hak pilih dari pemilih apakah telah memberikan hak suaranya ataau belum. Jika persyaratan telah terpenuhi maka sistem akan langsung membuat sebuah data *hash* dari nomor urut kandidat yang dimasukan oleh pemilih yang nantinya akan diberikan tanda tangan digital dengan menggunakan *private key* dari alamat *ethereum* pemilih, sehingga *smart-contract* dapat memastikan bahwa yang mengirimkan data untuk di simpan di dalam *smart-contract* adalah pemilih yang sudah terdaftar sebelumnya.



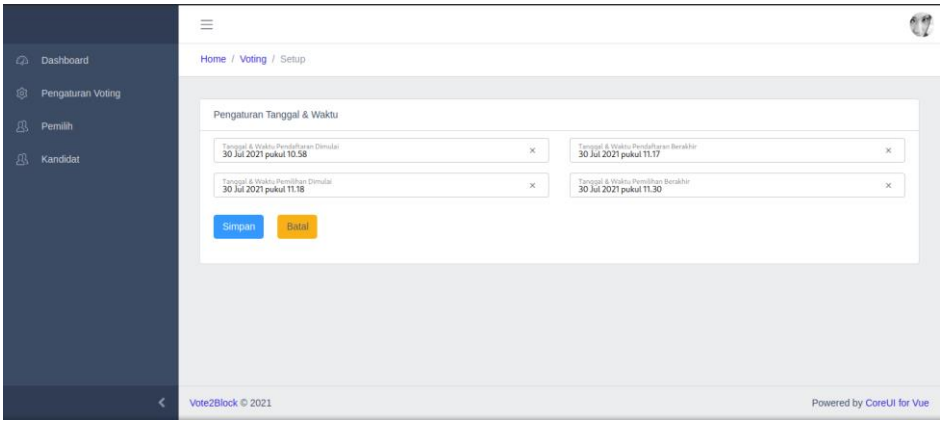
Gambar 5. Flowchart Proses Pemilihan

2.2 Rancangan Umum Sistem

Perancangan antarmuka atau *interface* dibuat dengan tujuan untuk mempermudah kerja pengembang dalam membangun sistem penelitian ini. Perancangan antarmuka berupa tampilan yang mudah dipahami. Tampilan *login* merupakan tampilan awal dari sistem *e-voting* dimana halaman *login* dibagi menjadi dua yang digunakan untuk pemilih dan *admin.* Tampilan halaman *login* dapat dilihat pada Gambar 6.

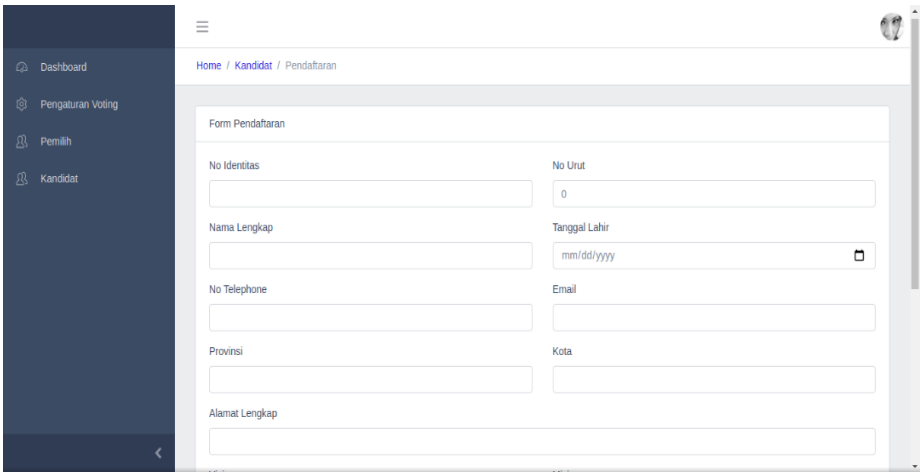
Gambar 6. Tampilan *login*

Sedangkan Tampilan *Dashboard Admin* akan ditampilkan jika *admin* berhasil masuk kedalam sistem *e-voting*, pada halaman *dashboard* ini hanya akan menampilkan *info card* dari jumlah total pemilih dan kandidat yang terdaftar dan juga jumlah *ethereum* yang dimiliki oleh sistem *e-voting*. Tampilan *dashboard admin* dapat dilihat pada Gambar 7

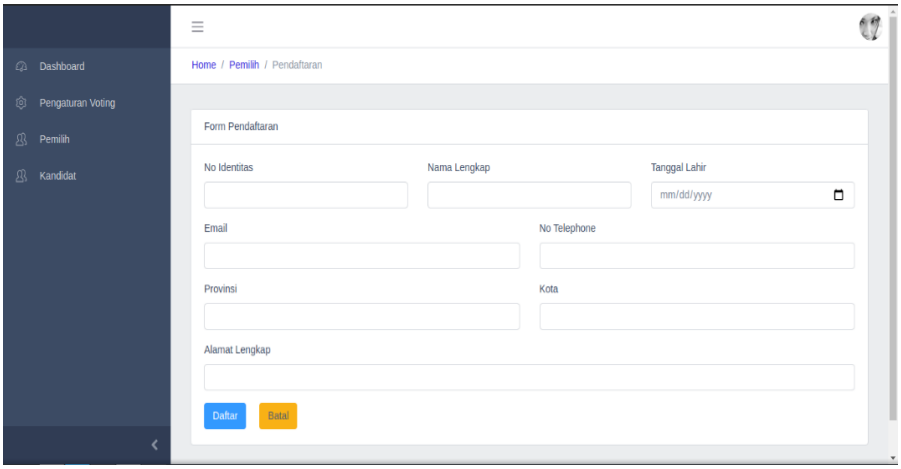


Gambar 7. Tampilan *login*

Pada Gambar 7 merupakan halaman *form* yang digunakan untuk mengatur waktu pendaftaran dan waktu pemilihan pada sistem *e-voting*. *Form* tersebut terdiri dari beberapa *input field* yang meminta pengguna untuk mengisi tanggal dan waktu dimulainya pendaftaran, tanggal dan waktu berakhirnya pendaftaran, tanggal dan waktu dimulainya pemilihan, dan tanggal dan waktu berakhirnya pemilihan. Halaman pengaturan waktu ini hanya dapat di akses oleh *admin* dari sistem *e-voting*.



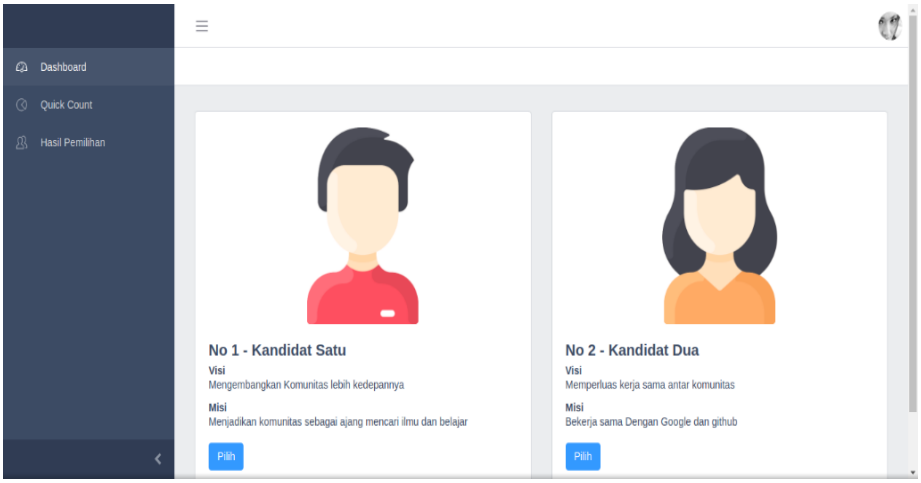
Gambar 8. Halaman pendaftaran kandidat



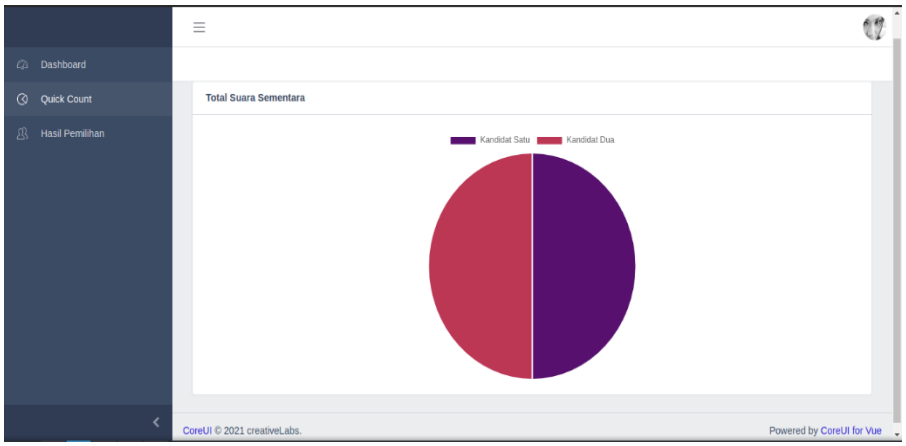
Gambar 9. Halaman pendaftaran pemilih

Pada Gambar 8 merupakan halaman pendaftaran kandidat yang digunakan oleh admin untuk mendaftarkan calon kandidat yang akan di pilih dalam proses pemilihan melalui sistem *e-voting*. Pada halaman pendaftaran tersebut, *admin* akan diminta untuk mengisi beberapa informasi dasar mengenai calod kandidat, seperti nama lengkap, foto kandidat, dan lainnya. Proses pendaftaran kandidat ini hanya bisa dilakukan ketika waktu pendaftaran telah dibuka sesuai dengan jadwal yang telah di tentukan sebelumnya.

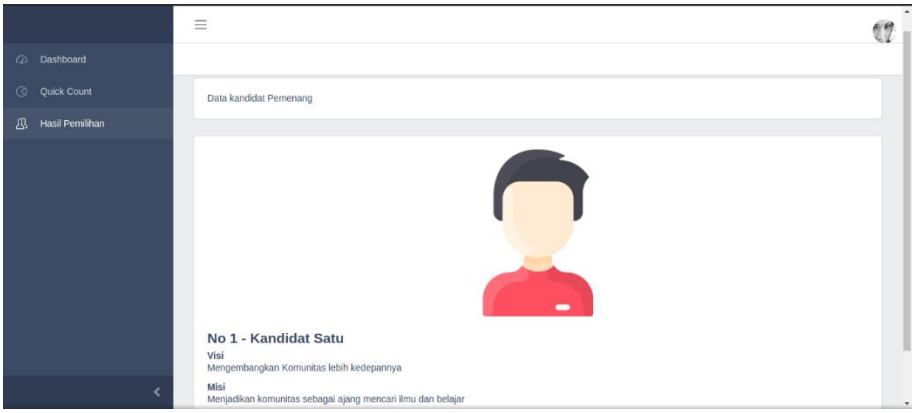
Pada Gambar 9 merupakan halaman pendaftaran pemilih yang digunakan oleh *admin* untuk mendaftarkan pemilihyang akan menggunakan sistem *e-voting* untuk memilih calon kandidatnya. Pada halaman tersebut, admin akan diminta untuk mengisi beberapa informasi dasar mengenai pemilih, sepertni nama lengkap, nomor identitas, alamat, dan lainnya. Proses pendaftaran ini juga hanya bisa dilakukan ketika waktu pendaftaran telah dibuka sesuai dengan jadwal yang telah ditentukan.



Gambar 10. Halaman pemilihan



Gambar 11. Halaman perhitungan sementara



Gambar 11.1 Halaman hasil pemilihan

Pada Gambar 10 merupakan halaman dimana pengguna dapat memilih kandidat yang terdaftar pada sistem *e-voting*. Pada halaman tersebut pemilih nantinya dapat melihat foto, nama lengkap, dan nomor urut kandidat. Pemilih juga dapat membaca profil singkat dari setiap kandidat, yang biasanya berisi informasi mengenai visi dan misi. Halaman pemilihan ini hanya akan tersedia untuk diakses ketika waktu pemilihan telah dibuka sesuai dengan jadwal yang telah ditentukan. Pada Gambar 10 merupakan halaman dimana pengguna dapat melihat total suara yang di dapatkan dari masing-masing kandidat selama proses pemilihan masih berlangsung. Gambar 11 merupakan halaman dimana pengguna dapat melihat kandidat yang berhasil memenangkan proses pemilihan.

3. HASIL DAN PEMBAHASAN

3.1 Uji Coba Sistem

Dalam penelitian ini, penggunaan metode white box testing, khususnya dengan teknik basis path testing, menunjukkan pendekatan yang cermat untuk memastikan keandalan dan keamanan smart contract dalam sistem e-voting. White box testing, sebagai metode yang melibatkan pemahaman mendalam terhadap struktur internal program, memberikan keunggulan dalam mengidentifikasi potensi kelemahan atau bug yang mungkin tidak terdeteksi dengan metode pengujian lain.

Metode basis path testing, yang berkaitan dengan perhitungan cyclomatic complexity, memberikan pandangan mendalam terhadap kompleksitas logis dari desain prosedural smart contract. Cyclomatic complexity menjadi indikator kritis dalam mengevaluasi sejauh mana program dapat diuji dan seberapa baik struktur kontrolnya dapat dipahami. Semakin tinggi cyclomatic complexity, semakin kompleks logika program, dan oleh karena itu, semakin penting untuk mencakup seluruh jalur independen dalam pengujian.

Pembuatan test case dari jalur independen yang didapat dari perhitungan cyclomatic complexity dan flowgraph sangat relevan. Hal ini memungkinkan peneliti untuk mengidentifikasi jalur yang memiliki potensi tinggi untuk menyebabkan masalah, baik dalam hal keamanan maupun keandalan. Dengan merinci setiap langkah dan kondisi pada setiap jalur independen, metode ini membantu memastikan bahwa setiap aspek dari smart contract telah diuji secara menyeluruh.

Namun, perlu diingat bahwa metode white box testing tidak dapat menangkap sepenuhnya semua potensi masalah yang mungkin terjadi pada level eksekusi nyata di lingkungan yang kompleks. Oleh karena itu, penting untuk melengkapi pengujian ini dengan metode black box testing yang mencakup skenario penggunaan yang beragam dan realistis. Kombinasi metode white box dan black box testing akan memberikan gambaran pengujian yang lebih holistik, menggabungkan keunggulan kedua metode tersebut untuk memastikan kehandalan dan keamanan sistem e-voting secara menyeluruh.

3.1.1 Pengujian White Box Tesing

Penerapan metode white box testing pada smart-contract pada gambar 12 yang akan digunakan di dalam sistem e-voting dengan menggunakan teknik basis path. Pada pengujian dengan menggunakan teknik basis path pengujian akan dilakukan dengan membuat sebuah test case yang didaptkan dari jalur independen, dimana jalur tersebut didapatkan dari perhitungan cyclomatic complexity dari sebuah flowgraph, flowgraph sendiri dibuat berdasarkan flowchart diagram dari smart-contract yang digunakan dalam sistem e-voting, pada gambar 12 adalah flowgraph yang akan dilakukan perhitungan cyclomatick complexity.

Analisis terhadap perhitungan cyclomatic complexity pada flowgraph (Gambar 10) menunjukkan bahwa nilai V(G) adalah 5. Cyclomatic complexity adalah suatu metrik yang digunakan untuk mengukur kompleksitas logika dari suatu program. Dalam konteks ini, V(G) mencerminkan jumlah jalur independen atau jalur eksekusi yang berbeda dalam flowgraph.

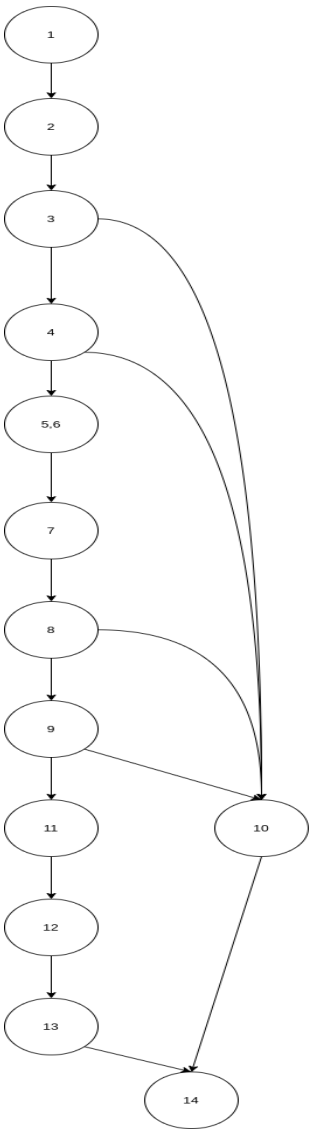
Pertama-tama, rumus cyclomatic complexity (V(G) = E - N + 2) dijelaskan dengan baik. E adalah jumlah edge (garis penghubung antar node), dan N adalah jumlah node dalam flowgraph. Dalam hal ini, perhitungan E, N, dan V(G) dilakukan berdasarkan flowgraph yang terkait dengan proses pemilihan.

Hasil perhitungan menunjukkan bahwa V(G) = 5. Artinya, terdapat lima jalur independen yang mungkin dalam flowgraph tersebut. Semakin tinggi nilai cyclomatic complexity, semakin kompleks logika program. Meskipun nilai 5 dapat dianggap sebagai tingkat kompleksitas yang sedang, perlu diingat bahwa semakin tinggi nilai cyclomatic complexity, semakin besar potensi kesulitan dalam pengujian dan pemeliharaan program.

Dalam konteks pengujian white box, nilai cyclomatic complexity yang lebih tinggi dapat menandakan bahwa lebih banyak skenario pengujian harus dipertimbangkan untuk mencakup semua jalur independen. Oleh karena itu, perhitungan ini memberikan pandangan yang berguna bagi pengujian untuk memastikan bahwa semua kemungkinan kondisi dan percabangan logika diuji secara menyeluruh.

Selain itu, hasil perhitungan cyclomatic complexity dapat digunakan untuk mengevaluasi kualitas desain program. Nilai yang tinggi dapat menunjukkan adanya kompleksitas yang berlebihan, dan dalam beberapa kasus, mungkin diperlukan refaktorisasi untuk meningkatkan keterbacaan dan pemeliharaan kode.

Secara keseluruhan, perhitungan cyclomatic complexity memberikan pemahaman yang berguna terhadap struktur dan kompleksitas logika dalam flowgraph proses pemilihan. Dengan nilai V(G) = 5, penelitian ini memasuki tingkat kompleksitas yang moderat, yang dapat diatasi dengan perencanaan pengujian yang cermat untuk mencakup semua jalur independen yang relevan.



Gambar 12. Flowgraph dari proses pemilihan

Berdasarkan dari flowgraph pada Gambar 10 dapat dilakukan perhitungan cyclomatic complexity dengan menggunakan rumus berikut:

$$V(G) = E - N + 2 \quad (1)$$

Dimana:
E = adalah jumlah dari edge atau garis penghubung antar node
N = adalah jumlah node yang terdapat di dalam flowgraph

Dengan menggunakan rumus tersebut dapat digunakan untuk menentukan jumlah jalur independent yang akan dilakukan pengujian, berikut ini adalah hasil perhitungan jumlah jalur independent dari flowgraph. Perhitungan cyclomatic complexity dari flowgraph proses pemilihan adalah.

$V(G) = 16 - 13 + 2$
$V(G) = 5$

Tabel 1. Data hasil pengujian proses pemilihan

No	Data Uji
1	kandidatPilihan = 1
2	pemilih_signature = 0xeb3ef6180e75d10699984aefb6331fde45fd1a8d91b290e403dc31e93ecfffb623e99923781fcf568a3812c97b775d2deabdc5b1a9217614cd481aca39c1906c1c
3	non_pemilih_signature = 0x228e7dabb08c20908c9199168a4338703ca697f355961af7c88e958c12ff2d466c5c97af18d2bd0366c6581f38be22508f5d1c09db6d7c6d061c5db5c97cb30d1c

3.1.2 Pengujian Black Box Tesing

Pada bagian ini akan dijabarkan mengenai pengujian fitur yang ada pada halaman proses pemilihan untuk melihat kesesuaian hasil uji coba dengan hasil yang diharapkan.

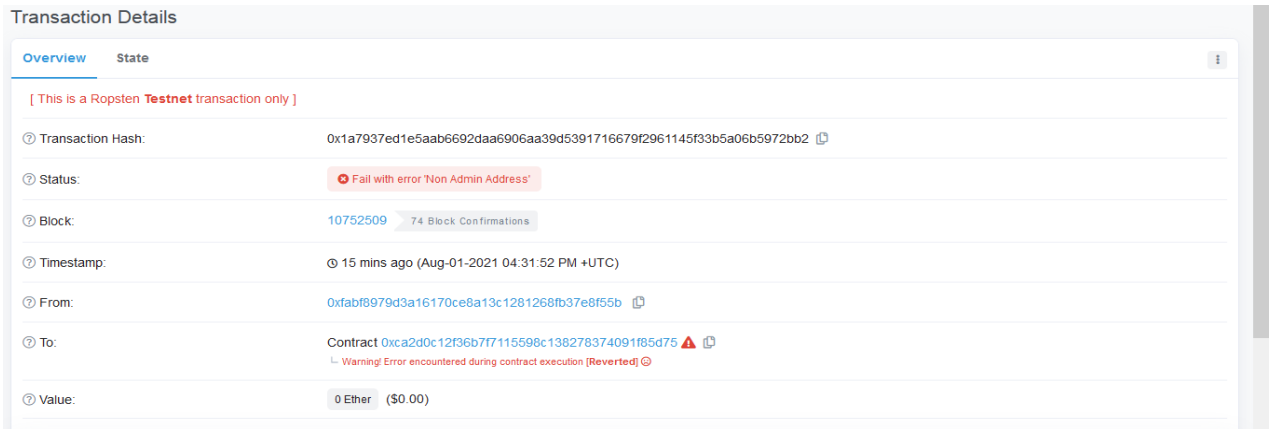
Tabel 2. Pengujian pada proses pemilihan

No	Langkah-Langkah	Hasil Yang Diharapkan	Hasil Pengujian
1	Membuka Halaman Dashboard Pemilih	Menampilkan Data Kandidat Yang Terdaftar	Sesuai
2	Klik Tombol Pilih Pada Salah Satu Kandidat	Menampilkan Pesan Berhasil, Dan Menampilkan Bukti Pemilihan	Sesuai

3.1 Pembahasan

Berdasarkan hasil implementasi dan pengujian adalah sistem e-voting berhasil dibuat berdasarkan dengan perancangan tampilan dan smart-contract yang dirancang untuk diterapkan pada sistem e-voting telah berjalan sesuai denga napa yang diharapkan, dimana smart-contract hanya dapat digunakan oleh admin dan pemilih yang telah terdaftar di dalam sistem e-voting. Sebagai contoh pada Gambar 11 dimana smart-contract akan melakukan penolakan proses penyimpanan data waktu pada sistem jika yang menjalankan bukan lah admin dari sistem e-voting tersebut.

Dapat dilihat pada Gambar 11 terdapat status fail error 'Non Admin Address' yang menandakan bahwa pengguna lain selain admin dari sistem e-voting berusaha untuk menambahkan data waktu kedalam smart-contract sehingga smart-contract secara otomatis akan melakukan penolakan untuk memproses penyimpanan data waktu, begitu juga dengan proses pendaftaran pemilih maupun kandidat, dan juga pada proses pemilihan dimana hanya pemilih yang telah terdaftar di dalam sistem lah yang dapat melakukan pemilihan.



Gambar 11. Penolakan penyimpanan data waktu

Sistem keamanan e-voting menggunakan arsitektur public blockchain ethereum yang di kembangkan dengan menerapkan smart-contract di dalamnya telah berhasil dibuat sesuai dengan perancangan tampilan, serta telah melakukan pengujian terhadap smart-contract, sehingga semua fungsi pada setiap fitur dapat berjalan dengan baik dan data dapat tersimban di dalam database serta smart-contract.

4. KESIMPULAN

Berdasarkan hasil penelitian sistem keamanan e-voting menggunakan arsitektur public blockchain ethereum dapat diperoleh kesimpulan bahwa smart-contract yang digunakan dalam sistem e-voting dapat digunakan untuk menjaga hasil pemilihan, dimana hasil pemilihan tersebut tidak dapat tambahkan atau dikurangkan, serta penggunaan alamat ethereum yang mewakilkan satu pemilih dapat menjaga privasi dari pemilih.

REFERENCES

[1] R. S. Bhadoria, A. P. Das, A. Bashar, and M. Zikria, "Implementing Blockchain-Based Traceable Certificates as Sustainable Technology in Democratic Elections," Electronics (Switzerland), vol. 11, no. 20, 2022, doi: 10.3390/electronics11203359.

[2] F. Baothman, K. Saeedi, K. Aljuhani, S. Alkatheri, M. Almeatani, and N. Alothman, "Computational intelligence approach for municipal council elections using blockchain," Intelligent Automation and Soft Computing, vol. 27, no. 3, 2021, doi: 10.32604/IASC.2021.014827.

[3] K. Tsomaia, A. Prangishvili, L. Imnaishvili, and M. Bedineishvili, "Blockchain-based biometric election system," International Journal of Circuits, Systems and Signal Processing, vol. 14, 2020, doi: 10.46300/9106.2020.14.13.

[4] A. M. Larriba, A. Cerdà I Cucó, J. M. Sempere, and D. López, "Distributed trust, a blockchain election scheme," Informatica (Netherlands), vol. 32, no. 2, 2021, doi: 10.15388/20-INFOR440.

[5] M. Kamil, A. S. Bist, U. Rahardja, N. P. L. Santoso, and M. Iqbal, "Covid-19: Implementation e-voting Blockchain Concept," International Journal of Artificial Intelligence Research, vol. 5, no. 1, 2021, doi: 10.29099/ijair.v5i1.173.

[6] Y. M. Wahab et al., "A Framework for Blockchain Based E-Voting System for Iraq," International Journal of Interactive Mobile Technologies, vol. 16, no. 10, 2022, doi: 10.3991/ijim.v16i10.30045.

[7] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, and M. Badra, "Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review," IEEE Access, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3187688.

[8] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, and G. Hjalmtysson, "Blockchain-Based E-Voting System," in IEEE International Conference on Cloud Computing, CLOUD, IEEE Computer Society, Sep. 2018, pp. 983–986. doi: 10.1109/CLOUD.2018.00151.

[9] S. Aggarwal and N. Kumar, "Blockchain 2.0: Smart contracts☆," in Advances in Computers, vol. 121, 2021. doi: 10.1016/bs.adcom.2020.08.015.

[10] K. Wisessing, P. Ekthammabordee, T. Surasak, S. C. H. Huang, and C. Preuksakarn, "The prototype of thai blockchain-based voting system," International Journal of Advanced Computer Science and Applications, vol. 11, no. 5, 2020, doi: 10.14569/IJACSA.2020.0110510.

[11] S. Prasetya Cahya and Inayatulloh, "Block chain model for regional elections in Indonesia," in Proceedings of 2020 International Conference on Information Management and Technology, ICIMTech 2020, 2020. doi: 10.1109/ICIMTech50083.2020.9211220.

[12] Y. C. Loke, N. K. Batcha, N. Sakinah, and N. S. B. N. A. Ziz, "Blockchain-Enabled Election Voting System," Journal of Applied Technology and Innovation, vol. 4, no. 4, 2020.

[13] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F. Y. Wang, "An Overview of Smart Contract: Architecture, Applications, and Future Trends," in IEEE Intelligent Vehicles Symposium, Proceedings, 2018. doi: 10.1109/IVS.2018.8500488.

[14] Z. Zheng et al., "An overview on smart contracts: Challenges, advances and platforms," Future Generation Computer Systems, vol. 105, 2020, doi: 10.1016/j.future.2019.12.019.

[15] G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, "On the Design and Implementation of a Blockchain Enabled E-Voting Application within IoT-Oriented Smart Cities," IEEE Access, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3061411.

[16] D. Lin, J. Wu, Q. Yuan, and Z. Zheng, "Modeling and Understanding Ethereum Transaction Records via a Complex Network Approach," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 67, no. 11, 2020, doi: 10.1109/TCSII.2020.2968376.

[17] T. Chen et al., "Understanding Ethereum via Graph Analysis," ACM Trans Internet Technol, vol. 20, no. 2, 2020, doi: 10.1145/3381036.

[18] M. Pawlak and A. Poniszewska-Marańda, "Trends in blockchain-based electronic voting systems," Inf Process Manag, vol. 58, no. 4, 2021, doi: 10.1016/j.ipm.2021.102595.

[19] S. Khan, A. Arshad, G. Mushtaq, A. Khalique, and T. Husein, "Implementation of Decentralized Blockchain E-voting," EAI Endorsed Transactions on Smart Cities, vol. 4, no. 10, 2020, doi: 10.4108/eai.13-7-2018.164859.

[20] S. A. Wright, "Towards a Blockchain Voting Roadmap," in 2021 3rd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2021, 2021. doi: 10.1109/BRAINS52497.2021.9569826.

[21] Y. S. Ihm and S. H. Kim, "Development of a Blockchain-Based Online Secret Electronic Voting System," IEICE Trans Inf Syst, vol. E105D, no. 8, 2022, doi: 10.1587/transinf.2021EDK0005.